Identified Security Requirements:

- Keeping the servers secure
- Keeping the 19th floor offices secure

Keeping the servers secure

1. The server will be kept on the 19th floor, which is leased by BCTAA. It will be kept in the private areas of the 19th floor, which is protected by a card reader door system. This would help to prevent visitors and unauthorised people from gaining access to the server as well as the network. In doing so, protecting unauthorised physical access to the server, which contains confidential client information.
2. The server is connected to the internet via a Wi-Fi router. The router contains a firewall and the latest cyber security technology to help protect the network. These can be setup and configured to reduce attacks from the internet as well as intrusion from attackers.

   The servers as well as Staff PC's are likely to be running an up to date operating system, such as Windows. This is an advantage, as the operating systems includes its own software firewall program, which will help to protect the machines from threats arising over the network. A firewall can be added to the server to protect it further from intrusion and attacks via the internet, which would limit the potential for attackers to gain access to the network.

3. The physical access routes to the network, such as Staff PC's, Router & Main Switch, are all located on the 19th floor. However, some staff can gain access to the network remotely through their Wi-Fi and mobile devices from home or client company locations, meaning they do not have to be present on the BCTAA premises to gain access to the network. Measures must be put in place to protect unauthorised access to the network, such as devices being plugged into the network through Ethernet ports and cables near the data outlets.

   BCTAA is on the 19th floor of a 20 storey building called Edexcelsior House, which has a mixed commercial and office usage, such as a gym on the ground floor, art gallery, restaurant and coffee bar on the 20th floor. These areas are open to the public. Therefore, there is the potential for visitors to go to the wrong floor, and may enter the 19th floor office premises. To protect against visitors gaining access to the BCTAA premises and to the network, measures could be put in place, such as login credentials and access rights on the network, to prevent the public from gaining access to Staff PC's.

4. To protect the server from intruders, the server will be hidden and won't show on the Wi-Fi network, in order to increase security.

5. NAT will be set up on the router, to allow remote access to the server. This is because BCTAA staff and visitors will need access to the server away from the

office premises. This would allow staff and visitors the opportunity to access the BCTAA network and server remotely through a VPN, as requested in the scenario plans.

Alternative Measures Could Include:

1. Installing/Configuring intrusion detection software so that it will monitor and produce reports of attempts to gain access to the server. This would allow BCTAA to be informed of potential attacks and unauthorised access to the server. This would run in conjunction with the network firewall.
2. Disabling/blocking unused data outlet point ports. These outlets and ports are connected to the network via cat 6 cable. To limit unauthorised devices from connecting to the network and gaining access to the server, port blockers can be installed to the unused ports, which can be locked and only removed with a key.
3. Improving and increasing physical security of the area which contains the network such as through biometrics such as iris scanners and finger print readers. This would limit access to the network area to only authorised BCTAA staff and technicians, as well as block potential visitors from gaining access.

I would recommend the first measure as it is highly achievable and possible to implement. The software would inform the company of attempts at trying to access the network and would allow for BCTAA to review its security measures and put newer, improved measured into place. However, this would require Baljinder or another member of staff to go through the reports and reviewing every attempts before assessing the dangers of them. This could increase staffing expense and as well as being time consuming. It is also worth noting that most intrusion attempts are pings and connection attempts that the firewall would frequently reject. This would add lots of data to the reports.

I would also recommend the second measure, as it is also achievable and can be implemented. Adding port blockers to the unused ports on the data outlet points mean that if someone needs to add their device to connect to the network, they will need the key or tool in order to remove the port blocker. This can be time consuming if this is necessary to connect their devices to the network in this way. It comes at a small expense to buy port blockers too.

The third measure would improve physical security of the premises, however it would increase the costs of BCTAA and would be costly to implement and maintain. Therefore, this option is costly.

Keeping the 19th floor secure

1. The whole of the 19th floor is to be leased by BCTAA. The whole floor contains internet access points, patch panels, electrical points and data outlet points. Currently, these are not secured, so the threat of these points being breached and allowing access to the network is high. The points are surrounded by controlled doors. To protect these points and limit attack,

these points could be moved to the more secure and private areas, which is controlled by a card system, hidden from sight, so that only authorised people can gain access and use these outlets. If this is not possible, the outlet points could be sealed/blocked off to prevent unauthorised access.

2. The scenario says the Edxcelsior Internet access system will be kept. Therefore, the cable connecting the Internet access point, Wi-Fi Router and Main Switch to each other will remain fibre optic. It is almost impossible to make an extra connection into fibre optic cable. This means that attackers are going to find it difficult to break into and attack the network. Another benefit of using fibre optic cables is that they are extremely resistant, as it is less likely to be affected by interference and signals, compared to other cables.

3. Devices connecting to the BCTAA network can connect through RJ45 such as Ethernet cables and fibre optic cables, whereas mobile devices such as laptops and smartphones will use Wi-Fi connection. It is therefore important that the Wi-Fi router is frequently updated and running the latest firmware, which is most secure and runs the most secure firewall. This is to prevent any attacking attempts from guests/visitors and staff. Important to ensure that the router is not on default settings and is using the most up to date password technology, WPA-2.

Alternative measures could include:

1. Improving the physical security of the floor by installing security doors on the whole 19th floor. This ensures only BCTAA staff and clients can access the office premises.

2. Improving the security of the premises by installing CCTV cameras to the floor, so that the behaviour and actions of passers-by can be monitored, and any suspicious behaviour can be flagged up and reported.

3. Improving the security of the offices by having an alarm system that sounds when someone enters the office. These alarms can be added to the entrances and to the controlled doors of the private areas. This can be configured so that it sounds only if someone doesn't touch in with their ID card or sounds when someone enters past the operating times of BCTAA. These measures can be implemented to prevent visitors from gaining access to the BCTAA offices, which would ensure that only staff along with clients can access the offices/floor.

The first measure would improve the physical security of the floor, however it would be expensive to implement and as BCTAA currently leases the floor, they would need

to seek permission from the Edexcelsior House management team, before being allowed to proceed with this measure. This would also prove time consuming and costly. Therefore, it may not be achievable and feasible to implement this measure.

The second measure would also improve the physical security of the floor, however it may be expensive to purchase CCTV cameras and install them all around the 19th floor. Modern CCTV's are connected via Wi-Fi to a network, therefore if they are not up to date in terms of software, it can be a vulnerability and provide an access point for attackers to gain access to a network. As a result, it may not be achievable and feasible to implement this measure.

The third measure would again improve the physical security of the floor. It is feasible to install this option, due to the fact that someone can gain access to the private areas with the push of the button from the inside. However, it could be costly to implement and install an alarm system onto the floor and office premises. The floor is likely to be packed with BCTAA workers every day, therefore having it sound every time someone enters may distract them and affect their productivity and focus. Therefore, the alarm system would not be utilised to its fullest.